



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/917,368	07/27/2001	Jeffrey Scott Bardsley	RSW920010137US1	1486
7590	01/11/2006		EXAMINER	
Duke Yee Yee & Assoiates P C 4100 Aiphia Road Suite 1100 Dallas, TX 75244			POPHAM, JEFFREY D	
			ART UNIT	PAPER NUMBER
			2137	
DATE MAILED: 01/11/2006				

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/917,368	BARDSLEY ET AL.	
	Examiner Jeffrey D. Popham	Art Unit 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 13 October 2005.

2a) This action is FINAL. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 5-11 and 15-27 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 5-11 and 15-27 is/are rejected.

7) Claim(s) _____ is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on 27 July 2001 is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
 Paper No(s)/Mail Date _____

4) Interview Summary (PTO-413)
 Paper No(s)/Mail Date. _____

5) Notice of Informal Patent Application (PTO-152)
 6) Other: _____

Remarks

Claims 5-11, and 15-27 are pending.

Response to Arguments

1. Applicant's arguments, see section II.A.2 of the remarks, filed 10/13/2005, with respect to the rejection(s) of claim(s) 5 under 35 U.S.C. 103(a) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made with Ricciulli (U.S. Patent 6,973,040) in view of Skirmont (U.S. Patent 6,553,005) and ND (Hunt et al., "Network Dispatcher: a connection router for scalable Internet services", 10/2/1998, Internet Security Systems, obtained from <http://www.unizh.ch/home/mazzo/reports/www7conf/fullpapers/1899/com1899.htm>).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 5-11, 15, and 18-27 are rejected under 35 U.S.C. 102(e) as being anticipated by Ricciulli (U.S. Patent 6,973,040).

Regarding Claim 5,

Ricciulli discloses a computer-implemented method of identifying the entry point of an attack upon a device protected by an intrusion detection system, the method comprising the steps of:

Obtaining intrusion information, from an intrusion detection system, regarding an attack upon a device protected by the intrusion detection system (Column 3, lines 16-33);

Obtaining network information, from network equipment connected to the device, regarding the attack (Column 4, line 45 to Column 5, line 2);

Determining a logical entry point (IP addresses, as well as TCP/UDP ports are logical representations used in combination to identify the entry point) of the attack using a correlation engine to correlate the intrusion information and the network information (Column 3, lines 16-43; and Column 4, line 45 to Column 5, line 2); and

Identifying a physical entry point (the physical entry point is where the router or node actually connects to the network, on its network interface) associated with the logical entry point (Column 3, lines 34-43).

Regarding Claim 6,

Ricciulli discloses that the intrusion information includes an address (Column 3, lines 16-33).

Regarding Claim 7,

Ricciulli discloses that the address is a source address (Column 4, line 65 to Column 5, line 2).

Regarding Claim 8,

Ricciulli discloses that the address is a destination address (Column 3, lines 16-33).

Regarding Claim 9,

Ricciulli discloses that the network information includes a logical port identifier of a logical port associated with the address (Column 4, line 65 to Column 5, line 2).

Regarding Claim 10,

Ricciulli discloses that the step of determining a logical entry point includes the step of finding, in the network information, the logical port identifier of the logical port associated with the address (Column 3, lines 29-43; and Column 4, line 45 to Column 5, line 2).

Regarding Claim 11,

Ricciulli discloses that the step of identifying a physical entry point includes the step of identifying a physical port associated with the logical port (Column 3, lines 34-43).

Regarding Claim 15,

Ricciulli discloses that the network equipment includes a firewall with routing function (Column 3, lines 16-28; and Column 4, lines 45-64).

Regarding Claim 18,

Ricciulli discloses that the intrusion detection equipment includes network based intrusion detection equipment (Column 5, lines 3-26).

Regarding Claim 19,

Ricciulli discloses that the intrusion detection equipment includes host based intrusion detection equipment (Column 3, lines 29-33).

Regarding Claim 20,

Ricciulli discloses that the intrusion detection system includes application based intrusion detection equipment (Column 5, lines 27-37).

Regarding Claim 21,

Ricciulli discloses a method of identifying the entry point of an attack upon a device protected by an intrusion detection system, the device being one of a plurality of devices connected by a network, the method comprising the computer-implemented steps of:

Detecting an attack on the device (Column 3, lines 16-33);

Notifying a correlation engine of the attack on the device (Column 3, lines 16-33);

Obtaining intrusion information regarding the attack (Column 3, lines 16-33);

Obtaining network information regarding the attack (Column 4, line 45 to Column 5, line 2);

Using the correlation engine, correlating the intrusion information and the network information to produce correlation information (Column 3, lines 16-43; and Column 4, line 45 to Column 5, line 2);

Using the correlation information, finding on the network a logical port of connection used by the attack (Column 3, lines 16-43; and Column 4, line 45 to Column 5, line 2); and

Mapping the logical port on the network to a physical port on the network using the correlation engine (Column 3, lines 34-43).

Regarding Claim 22,

Ricciulli discloses alerting a network manager to the location of the logical port and of the physical port (Column 3, lines 48-50).

Regarding Claim 23,

Ricciulli discloses that the step of mapping is performed using the correlation engine (Column 3, lines 34-43).

Regarding Claim 24,

Ricciulli discloses that the intrusion information includes an address (Column 3, lines 16-33); and the network information includes a logical port identifier of a logical port associated with the address (Column 4, line 65 to Column 5, line 2).

Regarding Claim 25,

Ricciulli discloses an apparatus for detecting a point of an attack on a network, the apparatus comprising:

Network equipment for connecting a protected device to a network (Column 3, lines 16-28);

An intrusion detection system comprising intrusion detection equipment (Column 3, lines 16-33);

A correlation engine (Column 3, lines 16-43; each of the system's routers contains this correlation engine, used to determine the entry point of an attack based upon stored and received information) adapted to:

- Receive a notification of an attack on the protected device (Column 3, lines 16-33);
- Receive intrusion information regarding the attack (Column 3, lines 16-33);
- Receive network information regarding the attack, wherein the network information pertains to the network (Column 4, line 45 to Column 5, line 2);
- Correlate the intrusion information and the network information to produce correlation information (Column 3, lines 16-43; and Column 4, line 45 to Column 5, line 2);
- Use the correlation information to find on the network a logical port of connection used by the attack (Column 3, lines 16-43; and Column 4, line 45 to Column 5, line 2); and
- Map the logical port on the network to a physical port on the network using the correlation engine (Column 3, lines 34-43).

Regarding Claim 26,

Ricciulli discloses means for alerting a network manager to the location of the logical port and the physical port (Column 3, lines 48-50).

Regarding Claim 27,

Ricciulli discloses that the intrusion information includes an address (Column 3, lines 16-33); and the network information includes a logical port identifier of a logical port associated with the address (Column 4, line 65 to Column 5, line 2).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ricciulli in view of ND (Hunt et al., "Network Dispatcher: a connection router for scalable Internet services", 10/2/1998, Internet Security Systems, obtained from <http://www.unizh.ch/home/mazzo/reports/www7conf/fullpapers/1899/com1899.htm>).

Ricciulli does not disclose that the network equipment includes a network dispatcher.

ND, however, discloses that the network equipment includes a network dispatcher (Pages 1-2, Introduction, Paragraphs 1-4). It would have been

obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the network dispatcher of ND into the intrusion detection system of Ricciulli in order to allow the system to protect a broader range of network equipment, thus increasing the types of routers that can be used and protected by the system, and to reach those customers that use network dispatchers.

4. Claims 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ricciulli in view of Skirmont (U.S. Patent 6,553,005).

Ricciulli does not disclose that the network equipment includes a load balancer.

Skirmont, however, discloses that the network equipment includes a load balancer (Column 5, lines 52-67). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the load balancing system of Skirmont into the intrusion detection system of Ricciulli in order to map packets that have a common source and destination by strict physical paths, while at the same time accomplishing efficient load balancing along the same physical paths, thus protecting against packets being received out of order, and consequently being lost/discarded (Column 1, lines 41-64; and Column 2, lines 20-50).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffrey D. Popham whose telephone number is (571)-272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Matthew Smithers
MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137